puresecurity™

Check Point SOFTWARE TECHNOLOGIES LTD.

Check Point SecureClient Mobile R65 HFA1 Release Notes & What's New

In This Document

Information About This Release page 1
What's New page 1
Software and Hardware Requirements page 1
Clarifications and Limitations page 3
Resolved Issues page 5
Frequently Asked Questions page 6

Information About This Release

This document contains important information not included in the documentation. Review this information before setting up SecureClient Mobile.

What's New

- SecureClient Mobile now supports Windows Mobile 6.0.
- Many resolved issues. See "Resolved Issues" on page 5 for more details.
- Interoperability with Pointsec Mobile.

Software and Hardware Requirements

In This Section

Supported Devices page 1
Unsupported Devices page 3
Supported Communication Cards page 3

Supported Devices

This section covers supported operating systems, processors, and tested devices.

Supported Operating Systems

- Any Pocket PC device running Windows Mobile 2003/2003 SE or Windows Mobile 5.0

Copyright © 2007 Check Point Software Technologies, Ltd. All rights reserved

- Any Smartphone device running Windows Mobile 5.0
- Any device running Windows Mobile 6.0 (classic, standard, professional)

Supported Processors

- Intel ARM/StrongARM/XScale/PXA Series Processor family
- Texas Instrument OMAP processor family.

Tested Devices

The devices in Table 1 have been tested and proved working.

Table 1 Tested Devices

Operating System	Tested Devices
PocketPC running Windows Mobile 2003/2003 SE	• HP/Compaq iPAQ Pocket PC 2003 - series 4150,4350,3950,5450, 5550, 2210,6340 • HP/Compaq iPAQ Pocket PC 2003 SE / Phone Edition - series 4700, hx2x00 • Dell AXIM X5 PocketPC 2003 • HTC Himalaya (XDA II, MDA II, Qtek 2020, i-Mate, Orange SPV1000) • HTC Blue Angel (XDA III, MDA III, Qtek 9090, i-Mate 2K, Sprint PPC-660, Verizon XV6600, Cingular SX66) • HTC Magician (Dopod 818, i-mate JAM, O2 Xda mini, Qtek 5100, MDA Compact)
PocketPC running Windows Mobile 5.0	• Dell AXIM X51v • HTC Universal (O2 Exec, i-Mate JasJar, Orange M5000, MDA IV) • HTC Wizard/Apache (Sprint PPC6700, Orange SPV M3000a, T-Mobile MDA Vario, i-mate K-Jam) • ETEN M600 • Palm Treo 700w, 700wx, 700v • HTC TyTN • Fujitsu Siemens LOOX T830
Hardened PocketPC devices	• Symbol MC70 • Motorola HC700 • Intermec 700
Windows Mobile 5.0 Smartphone	• HTC Tornado (i-mate sp5/sp5m, qtek 8310 • HTC StrTrk (i-mate smartflip, qtek 8500, Cingular 3125) • Motorola Q • HTC S620 (Excalibur, t-mobile Dash) • Samsung i320, i600
Windows Mobile 6.0 (Classic/Professional)	• PPC6800 • HTC Touch • HTC s710/VOX

Unsupported Devices

- HP iPaq 6900 series (however, a patch is available - see SecureKnowledge SK #32505).
- HP Thin Client devices.
- HTC Advantage X7500/X7501. (Client User interface is distorted).
- Toshiba portégé g900. (Client User interface is distorted).

Supported Communication Cards

Any card that supports the supported devices and provides an IP interface should be valid.

The following cards have also been tested and proved working

- TRENDNet TE-CF100 10/100MBps CompactFlash Fast Ethernet Adapter
- Socket Communications CF Wireless LAN Card
- Linksys WCF 12
- Sierra AirCard 750
- Sierra AirCard 555
- SanDisk Connect Wi-Fi SD Card
- Socket Communications CF Bluetooth Adapter
- Socket Communications Serial Adapter
- Spectec WLAN-11b

Clarifications and Limitations

1. Task Manager applications, like WizbarLite, Spb Pocket Plus and HTC Task Manager should not use the [x] option to close the SecureClient mobile application. Terminate the application instead of minimizing it. SecureClient Mobile should be added to the “excluded applications” for this feature, or the feature should be turned off.
2. On the HP PocketPC series, the iPAQ Wireless application and today item malfunction when SecureClient Mobile is installed. A patch is available through SecureKnowledge database. See SK #32505.
3. When installing the client on Windows Mobile 5.0 PPC, a warning message is issued stating the application is not signed.

   The executables and package are signed with a Check Point certificate. One can install the `cpcert.cab` provided in the ZIP package before installing the client to prevent this warning.
4. When installing the client on a PocketPC 2003 device, it is required to install the unsigned package `SecureClient_Mobile_Setup_626000xxx_unsigned.cab`.

   This is an operating system limitation.
5. When working with certificates authentication, make sure there is only one valid certificate for the relevant gateway in the CAPI store. In case more than one such certificate exists, the first one is used without prompting the client to choose which certificate to use (as done by Internet Explorer).
6. Installing the client to a storage card is not supported.
7. On some devices, an error message with the AcquireCredentialsHandle is mentioned. In most cases this issue is resolved by quitting the client and restarting it. In some cases a soft-reset is required.

8. Connecting through a proxy that requires digest authentication is not supported. NTLM authentication is also not supported.
9. Certificate enrollment (CheckPoint CA), a feature that is implemented on both SecureClient and SNX is not supported on this client release. When "Certificate with enrollment" is selected in SmartDashboard and the user does not have a valid certificate in its CAPI store, the result is that the user receives an error message.
10. When the client is installed but not running on a Windows Mobile 5.0 device, ActiveSync is disabled. To over come this, start the client, then start the ActiveSync. Since the client is not running, a change in the fireWall policy required for the ActiveSync protocol to run cannot be applied.
11. When using WM5.0, there are cases where the uninstalling/upgrading the client failed. In such a case, the client loads with an error message stating that the client drivers did not load. A second uninstall removes the client completely in such a case.
12. When using SCM and SSL Network Extender with RADIUS authentication and `ipassignment.conf` for Office Mode, the proper IP addresses are not assigned resulting in failed connections.

    For a patch to earlier gateway versions please open a Service Request with Check Point support.
13. On some Windows Mobile 5.0 devices when connecting to the gateway over ActiveSync (used as network interface) TCP connections and targeting resources behind the gateway, do not open over the tunnel, usually, resulting with a timeout. This is caused by the DTPT LSP "hijacking" all TCP connections and bypassing the routing table.

    The workaround available is to change the ActiveSync connection type from RNDIS to Serial. To do this uncheck the **Enable advanced network functionality** in the 'USB to PC' applet in the device network settings. (This option exists in most WM50 aku2 and above devices).
14. The flag `neo_policy_expire` should be configured to request for the client to update its policy regularly. The following flags are not implemented: `neo_enable_automatic_policy_update` and `neo_automatic_policy_update_frequency`.
15. Changing the value `neo_remember_user_password` to `true` becomes operative on the client only after the second login, after the flag was downloaded to the client. The client is updated with the new policy and only in the subsequent login it actually saves the password.
16. The device issues DNS queries on both the physical and virtual interfaces which could expose server names and IP addresses. To prevent this, set the flag `neo_allow_clear_while_disconnected` to `false`.
17. MSI installer does not enforce that upgrading should only be done to a higher build number. On the device, when the CAB file is installed this enforcement does take place.
18. If setting the Office Mode pool to high address numbers, for example 230.230.230.0, the users will not be able to connect. A message will appear:

    > "Client Disconnected: (44) Failed to apply assigned office Mode IP data. If this problem persists you should reset your device."

    This is an invalid Office Mode configuration for all of the Check Point VPN clients.
19. A user that is authenticating using user-password scheme and wants to switch to certificate authentication must clear its cached credentials. This is done on the client: **Menu > Options > Clear_passwords**.
20. Changing the gateway from SSL Network Extender mode only (`snx_enabled`) to SCM mode only might cause the client to stop downloading a policy from the server, even if SCM mode (`neo_enable`) is operative.

21. The client does not support Connectra's Nextwork Extender Application Mode. When setting Connectra to Application Mode the client's connection fails with the error message "authentication failure (201)".
22. The flag `NEOGUI_NO_GUI` is not fully supported. The client has to be restarted for the flag to take effect (the flag should be set before the client's GUI is initialized). The flag `NEOGUI_NO_OPTIONS_DLG` is not implemented in this client release.
23. Some of the SSL Network Extender (SNX) settings conflict with SecureClient Mobile (SCM) settings. The following flags take precedence when SNX and SCM are both enabled on the same gateway (all are found both in the SNX dialog under **Global Properties > Remote Access** and on the **SecureClient Mobile** dialog:
    - User authentication method: snx_user_auth_methods over user_auth_methods
    - Re-authenticate user every: snx_user_re_auth_timeout over neo_user_re_auth_timeout
    - Supported encryption methods: snx_encryption_methods over neo_encryption_methods
    - Send keep-alive packets every: snx_keep_alive_timeout over neo_keep_alive_timeout
24. When the "HTTP methods" option is enabled in the Connectra web intelligence page, Microsoft ActiveSync synchronization with Exchange server fails. The workaround is to disable "HTTP methods" protection in the above page.
25. MSI installer does not support Windows Vista. Client is not installed on the device and no error message is generated.
26. RSA SoftID v2.2 is not supported by the client. Use v2.0.
27. SecureClient Mobile Licenses are not added to a VPN gateway. Users need to obtain an SSL Network Extender license instead. For more information, see sk33491.
28. If you change the IP forwarding policy, the policy will not take effect until after the next device reset. However, if the device is reset immediately the policy may be lost. Changing the IP forwarding setting results in a registry key modification on the Secure Mobile device. For performance reasons, the device's system registry is loaded into memory and changes periodically flushed to persistent storage. If the user soft resets a device or removes a battery during the period of time between a registry value changing and those changes being flushed, the changes will be lost when the device is tuned back on. For this reason, a Secure mobile device whose downloaded policy prevents IP forwarding may still be capable of IP forwarding.

Smartphone

29. When running the CertImport utility the selection of the certificate should be done using the [select] key and not by the joystick's center-click. Selecting the certificate with the joystick results with the operating system trying to "run" the certificate and an error message.
30. Smartphone devices are unable to connect over ActiveSync to a PC. There's currently no workaround.
31. The proxy replacement feature is not functional.
32. When the client is connected on some models the VNA is falsely identified as WiFi interface in home plug-in.

Resolved Issues

1. On Smartphone devices, when the user inserted symbols using the [*] key, the dialogs were refreshed and data deleted. User can now insert symbols to authentication dialogs.
2. On some Smartphone models, the home-screen was corrupted when the **Show Today Item** checkbox was selected.

3. SAA plug-ins now work with Connectra challenge-response authentication.
4. API and CLI no longer fails when the device is out of the cradle.
5. Improved client stability
6. One some device models, SecureClient Mobile is able to connect when debug-logging is turned on.
7. SecureClient mobile now works on Intermec 700 devices.

Frequently Asked Questions

Question: I cannot connect to my gateway.

Answer: Check the following on the Gateway:

- SCM license is installed.
- The user is valid for current date (under the users tab in the SDB).
- In SmartDashboard, click **Manage > Users and Administrators**. Select the user and click **Edit**. In the **Encryption** tab, make sure that the user has the **IKE** checkbox checked.

On the client:

- Check that the user has a valid certificate and that the certificate has been installed on the client (via the Cert_import utility supplied with the client.) This certificate is the sole "personal" certificate that matches the requested server (check under **Start > Settings > System** tab **> Certificates**).
- The gateway certificate can be validated by a root CA on the device. Try connecting to the gateway with Pocket IE (e.g. to https://myserver.com) to get some more info on the certificates validation done.

Question: I am able to connect and access the Intranet using Internet Explorer, but unable to read mail using my IMAP account.

Answer: In the Messaging application, go to **Tools > Accounts**. Choose your e-mail account to edit it. Click **Next** and go into **Options**. In the **Connection** drop-down box, choose **Work**.

Question: Does Integrity Clientless Security (ICS) and Integrity Secure Browser (ISB) supported by the Windows Mobile device?

Answer: Currently, ICS and ISB are not supported over Windows Mobile devices.

Customers that wish to use the client with VPN1/Connectra gateway will require not to enforce ICS/ISB.

Question: My gateway enforces Secure Configuration Verification (SCV) and it drops the client traffic packets. Is there a workaround?

Answer: Allowing access to SSL clients on gateways enforcing SCV is a new feature that was added to R65 gateways and management (also available on VPN1 gateways in R60 HFA6, R61 HFA2 R62 HFA1). To enable this option on SmartDashboard go to **Global Properties > Remote Access > SCV > Exceptions**. On R55 use the procedure described in SK #30789 - SNX client traffic dropped when SCV is enforced.

Question: What are my options for configuring the client to Route All Traffic through Gateway ("Hub Mode", "VPN Routing")?

Answer: There are two issues here:

a. How do I configure the client to make the device route all its traffic through the VPN tunnel when connected. The options are: (a) Configure the encryption domain to include "the whole world" (network 0.0.0.1-255.255.255.254). This is described in SK #31367. Note that since NGX R60, the remote access encryption domain can be set to a different one than the gateway to gateway encryption domain. (b) Configure the client to route all its traffic through the gateway using the `neo_route_all_traffic_through_gateway` flag.

b. How do I prevent the device from accessing the Internet when the VPN tunnel is not connected? Set up the client firewall to enforce **Encrypted Only** policy. This prevents any traffic coming into the device or going out of the device that is not going through a VPN tunnel.

Question: I have enabled **Route all traffic through gateway** (in the client options dialog) but all traffic destined to outside of the corporate network is dropped by the gateway.

Answer: When using a gateway that was not upgraded to support SecureClient Mobile (patch) and that is not configured with a Remote Access encryption domain that includes "the whole world", as described in A7, you have to turn on a global flag `GW_route_traffic_for_OM_address` to true using GuiDBEdit. Note that this flag will allow all remote access clients to route their traffic through the gateway.

Question: Why does the client installer disable the AutoBind LSP in WM 5.0? What effect would it have?

Answer: The Auto Bind feature, introduced in WM 5.0, conflicts with the Office Mode feature of the client (the virtual interface that is assigned a private address by the connected gateway) because it makes several applications on the device ignore the IP routing table, needed for VPN routing.

More info on the issue can be read in the following links:

http://www.codecomments.com/message2290664.htm

http://blogs.msdn.com/cenet/archive/2005/10/25/484936.aspx

http://www.intrinsyc.com/whitepapers/RIL_whitepaper_MS_Intrinsyc_June2004.pdf

Question: Is it possible to disable the sound effects the client produces when connecting and disconnecting?

Answer: Rename the folder `Sound` found in `Program Files\CheckPoint\Neo` to `Sound.bak`.

Question: Can the Client run on WinCE 4.2? What about WinCE.Net or CE 5.0?

Answer: WinCE 4.2 is the underlying OS for PocketPC 2003/SE and SmartPhone 2003.

There are many devices running WinCE that are not PocketPC/SmartPhone. If the device is a PocketPC/SmartPhone, it is supported. WinCE.NET is an acronym for WinCE 4.2. CE 5.0 is an acronym for Windows Mobile 5.0. The current client supports any PocketPC/SmartPhone that is running Windows Mobile 5.0.

Question: How can I collect the client logs if I cannot start the client or the client is stuck or the Troubleshooting Dialog is not accessible to me?

Answer: To enable the client logging (if the troubleshooting page doesn't work) use any registry editor (e.g. TascalRegEdit - <http://www2r.biglobe.ne.jp/~tascal/download/pocketpc/tre_e.htm>) and set the registry value `HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\Neo\Debug\client_log` to `1`. Restart the client process. If it is stuck, stop as follows:

1. Tap **Start > Settings > System** tab**> Memory > Running Programs** tab.
2. Highlight the program and tap **Stop**.

Question: What license is needed for SecureClient Mobile?

Answer: Both Connectra and VPN-1 gateways require a license for SecureClient Mobile. The license is installed on SmartCenter server, and contains one of the following SKU's, depending on the number of concurrent connected users requested:

- #115043 CPVP-SCM-25
- #115044 CPVP-SCM-100
- #115046 CPVP-SCM-250
- #115047 CPVP-SCM-500
- #115048 CPVP-SCM-1000
- #115049 CPVP-SCM-5000
- Evaluation license: CPVP-EVAL-SCM-25-30/1

Question: I have SecureClient licenses that are not in use and I would like to exchange them for SecureClient Mobile licenses. Is it possible to do this? Discount?

Answer: Yes. An upgrade path is available with 80% off. Access the Check Point User Center and ask for license exchange.

Question: After installing an HFA on the module I tried to connect the client for the first time. The client connects OK but the policies do not seem to be downloaded to the client. What might have gone wrong?

Answer: After installing the HFA one further "manual" step is needed in most cases. When HFA is installed it does not override any existing configuration files. Instead, the configuration files are copied to the `conf` folder with an "`_HFA`" appended to the file name. Such configuration files should be manually renamed after copying any relevant configuration data into them. There are 3 configuration files that are part of the SCM support and should be renamed:
`$FWDIR/conf/*_HFA.ttm => $FWDIR/conf/*.ttm`

Question: What Management patch should I install on Provider-1 and on SmartCenter prior to R65 so that SecureClient Mobile configuration is available in the database?

Answer: Refer to #sk32210,

Question: What is the expected performance for the VPN client?

Answer: The expected performance varies considerably depending on several parameters. Here are some test results for VPN throughput over WiFi (802.1b) - comparing clear traffic to traffic over the connected VPN client. Tested with client build 240 on HP iPaq HX-2790 downloading a 5.15MB file over HTTP:

- Http in clear: 17sec => 310.1 KB/Sec
- Http over SCM: 33sec => 159.8 KB/Sec

Question: Why do I have to install `cpcert.cab` first, before installing the SecureClient Mobile cab on the Smartphone? Why doesn't checkpoint sign the client package with a trusted Verisign certificate?

Answer: Most Smartphones come locked. Check Point certificates must be installed on the device (once) before attempting to install SCM. The certificates installer is found in the client distribution ZIP file under `smartphone_unlock/cpcert.cab`. Note that this may apply to WM50 Pocket Pc devices even though they mostly come unlocked.

Signing the package with a Verisign certificate is not enough, all executables must be signed as well. This makes the signing process impractical and the ability to update the client, release HFAs and customer patches more expensive.

In most cases having the client signed by Verisign will not make a difference anyway, since most administrators customize their package. Package customization changes the CAB so that it has to be signed again. An administrator can sign the new CAB with a Verisign certificate. In any case, `cpcert.cab` must be installed only ONCE on each device so that "trust" for Checkpoint software is accomplished. Later on, there is no need to install cpcert.cab again on upgrades and additional Check Point software.

Question: What is the amount of traffic produced by the client (keep-alive) mechanisms when running in Always-Connected?

Answer: The calculation shows that the always-connected overhead on traffic is about 30MB a month when using standard settings (Keep-Alive every 20 seconds). One can reduce this number significantly by reducing keep-alive timeout. Reducing it to once every 40 seconds should have no noticeable effect in most cases (set neo_keep_alive_timeout to 40). When running MS Direct-Push on-top of the VPN tunnel, one can set this flag to 300 (once every 5 minutes), since the Direct-Push protocol has a keep-alive mechanism of its own.

Question: When I try accessing my Intranet website, using PocketIE over the connected client, I am continuously prompted for authentication. Why is that?

Answer: Many intranet websites require NTML authentication that is not supported by Pocket IE. Install minimo (Firfox for PocketPC) to overcome this limitation.
http://www.mozilla.org/projects/minimo/

Question: Are there any advantages to connecting to VPN1 gateway (R65) over Connectra Gateway (R65CCM)?

Answer: There are a few limitations when terminating the client on a Connectra gateway:

a. You cannot enable mobile devices without enabling SNX as well (Windows' SSL Network Extender/SNX). This may be a major problem considering that SCM does not support ICS. That is, you have a gateway that is accessible by Windows SNX that is not going through ICS checks.

b. On a VPN-1 gateway both the authentication "channel" and the data "channel" are on a single server (one IP address and port). On a Connectra gateway these "channels" cannot share one address/port. That is, you need a second IP address or a second port (default is a second port - 444).

c. Connectra has no inherent 'route traffic through gateway' feature. For this reason, enabling route-all-traffic-through-gateway (hub Mode) for clients using Connectra is somewhat tricky and limited.

d. Connectra is not meant to be used as a perimeter gateway, but as a remote access gateway in the DMZ.

e. Client upgrade (if needed) is done after client authentication.

f. SAA plug-in DLLs must be configured in the client package, if it is not based on a textual challenge-response.

In addition, there are limitations when terminating the client on a VPN-1 gateway. The following represent the limitations when using SecuRemote/SecureClient in conjunction with SecureClient Mobile on the same gateways:

a. If you have a few gateways that are used for remote access with SecuRemote/SecureClient and they are NOT in full MEP configuration (full overlapping encryption domain), you cannot use any of them to terminate SCM. This occurs because the encryption domain SCM only sees the connected gateway. For this reason, so it will not be able to access resources behind other gateways.

b. Is it possible to add a new VPN-1 gateway that will only terminate SCM? NO! All the VPN-1 gateways share the same Remote Access Community. This means that once you add a new gateway the encryption domain seen by SecuRemote/SecureClient becomes corrupt/illegal and the clients will not work. You can add a new stand-alone gateway (different Smart Center => different Remote Access Domain).

Question: Are there any tricks that will allow connecting to Connectra with the GuiDBEdit tool? I know its possible from the local command line and I was wondering if there was a way to do this with the GUI since you cannot define GUI clients?

Answer: To connect to Conectra with the GuiDBEdit tool perform the following:

a. Open an SSH connection to the Connectra gateway/

b. Define the environment variable `OPEN_CPMI_SERVER_PORT`:

```
>setenv OPEN_CPMI_SERVER_PORT 1
```

c. Define the environment variable `EXPOSE_HIDDEN_OPTIONS`:

```
>setenv EXPOSE_HIDDEN_OPTIONS 1
```

d. Run cpconfig and add a GUI administrator:

```
>cpconfig
```

Select option 2 (administrators), Type a username and a password, with all permissions.

e. From `cpconfig`, add a GUI client:

Select option 3 (GUI clients), Any, Ctrl-D, y

f. Perform a `cprestart` so the settings above take effect.

g. On the client's machine, install the appropriate SmartDashboard version. Please choose a machine on which SecureClient is not installed:

- For Connectra NGX R60 and earlier: SmartDashboard NG R55
- For Connectra NGX R61 and later: SmartDashboard NGX R60

h. Backup and replace `CPMIClient501.dll` and `CPMIBase501.dll` in the SmartDashboard installation path (`c:\Program Files\CheckPoint\SmartConsole\Rxx\Program`) with the following files:

- Connectra 2.0
- Connectra NGX R60
- Connectra NGX R61 (only GuiDBEdit will work)

i. Run SmartDashboard and connect using the chosen GUI admin, username and password.

Question: Where can I access additional information about Windows Mobile 5.0 Application Security?

Answer: You can find additional information in the following location:
http://msdn2.microsoft.com/en-us/library/ms839681.aspx

Question: Is there a simple tool that I can use to run pings, trace-routes, lookups etc., on the mobile device?

Answer: Try VxUtil. You can find this tool in the following location:
http://www.cam.com/vxutil_pers.html

Question: Can I move the Email and Attachments to a Storage Card? What about the IE cache?

Answer: For information refer to http://www.frode.cc/ or use a tool such as Oldsap's OS RegTweaker.